POWERED BY Dialog

Network security system for wireless communication networks, has controller that extracts non-registered access points by comparing list of previously registered access points with lists dispatched by clients

Patent Assignee: IBM CORP; INT BUSINESS MACHINES CORP
Inventors: FUJII K; ITO M; ITOH M; MATSUNAGA K

Patent Family (3 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20030117985	A1	20030626	US 2002248116	A	20021219	200362	B
JP 2003198571	A	20030711	JP 2001395303	A	20011226	200362	E
JP 3792154	B2	20060705	JP 2001395303	A	20011226	200644	E

Priority Application Number (Number Kind Date): JP 2001395303 A 20011226

Patent Details

Patent Number	Kind	Language	Pages	Drawings	Filing Notes
US 20030117985	A1	EN	14	7	
JP 2003198571	A	JA	11		
JP 3792154	B2	JA	14		Previously issued patent JP 2003198571

Alerting Abstract: US A1

NOVELTY - The system has clients (10a-e) that search for neighbor access points in order to establish wireless connection to a local area network (LAN) and dispatch a list of access points obtained to a controller (20), as a result of the search. The controller extracts non- registered access points by comparing a list of previously registered access points with the lists dispatched by the clients.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1.an access point recognizing method 2.a method of checking an access point.

USE - Used for wireless commun ication networks.

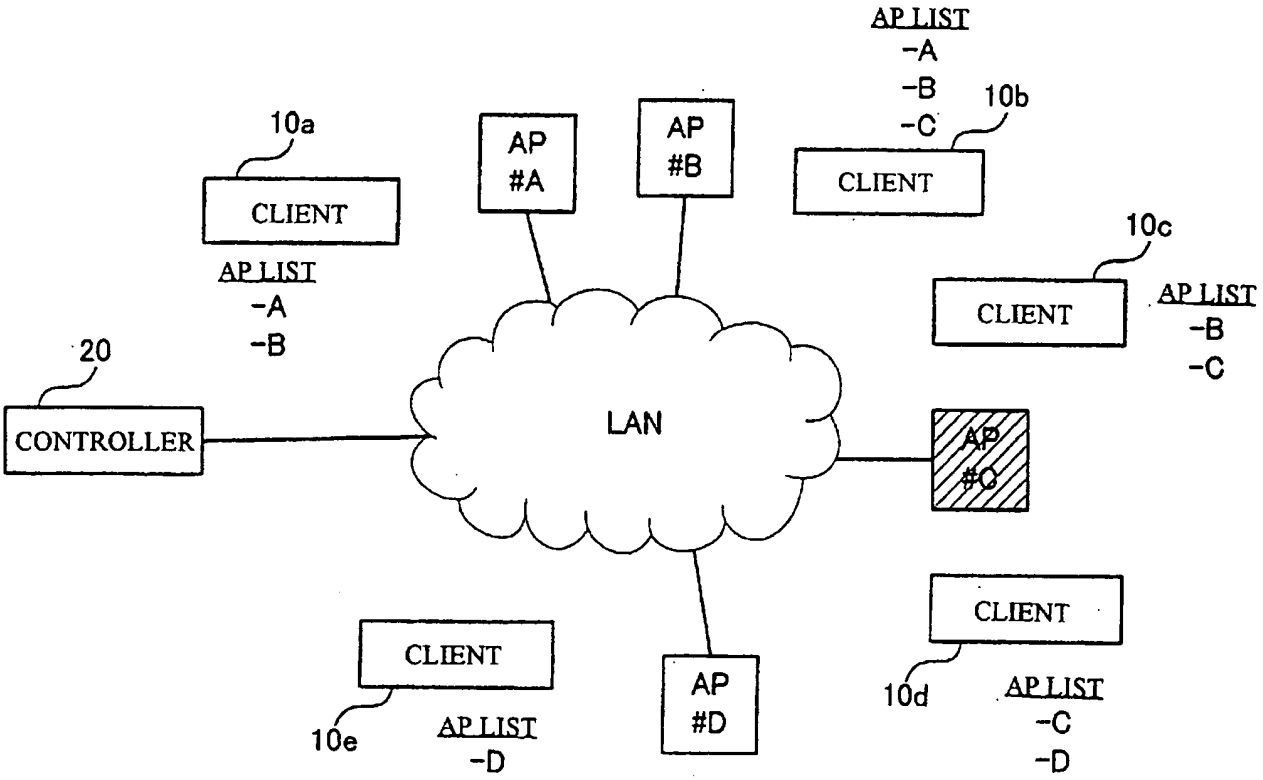
ADVANTAGE - The apparatus can detect illegal access p oints within the network according to the information on the retrieved access points, thereby enhancing security in the network.

DESCRIPTION O F DRAWINGS - The drawing shows a configuration of a local area network system.

10a-e Clients

20 Computer.

Main Drawing Sheet(s) or Clipped Structure(s)



International Classification (Main): H04L-012/28 **(Additional/Secondary):** G06F-013/00, H04Q-007/38

International Patent Classification

IPC	Level	Value	Position	Status	Version
H04L-0012/28	A	I		R	20060101
H04L-0012/28	A	I	F	B	20060101
H04L-0029/06	A	I		R	20060101
H04Q-0007/38	A	I	L	B	20060101
H04L-0012/28	C	I		R	20060101
H04L-0029/06	C	I		R	20060101

US Classification, Issued: 370328000, 370338000

Original Publication Data by Authority

Japan
Publication Number: JP 2003198571 A (Update 200362 E)

Publication Date: 20030711
NETWORK SECURITY SYSTEM, COMPUTER SYSTEM, RECOGNIZING PROCESSING METHOD FOR ACCESS POINT, CHECK METHOD FOR ACCESS POINT, PROGRAM, STORAGE MEDIUM AND DEVICE FOR WIRELESS LAN
Assignee: INTERNATL BUSINESS MACH CORP (IBMC)
Inventor: FUJII KAZUO MATSUNAGA KOZO ITO MASAHARU
Language: JA (11 pages)
Application: JP 2001395303 A 20011226 (Local application)
Original IPC: H04L-12/28(A) G06F-13/00(B) H04Q-7/38(B)
Current IPC: H04L-12/28(A) G06F-13/00(B) H04Q-7/38(B)|JP 3792154 B2 (Update 200644 E)
Publication Date: 20060705
Assignee: IBM CORP (IBMC)
Language: JA (14 pages)
Application: JP 2001395303 A 20011226 (Local application)
Related Publication: JP 2003198571 A (Previously issued patent)
Original IPC: H04L-12/28(B,I,H,JP,20060101,20060615,A,F) H04Q-7/38 (B,I,H,JP,20060101,20060615,A,L)
Current IPC: H04L-12/28(B,I,H,JP,20060101,20060615,A,F) H04Q-7/38 (B,I,H,JP,20060101,20060615,A,L)

United States
Publication Number: US 20030117985 A1 (Update 200362 B)
Publication Date: 20030626
NETWORK SECURITY SYSTEM, COMPUTER, ACCESS POINT RECOGNIZING METHOD, ACCESS POINT CHECKING METHOD, PROGRAM, STORAGE MEDIUM, AND WIRELESS LAN DEVICE
Assignee: INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, 10504 New York, US (IBMC)
Inventor: FUJII, KAZUO, 1951-41, Tohkaichiba-Midori-ku, Yokohama-shi, Kanagawa-ken, JP Nationality: JP ITOH, MASAHARU, 5-3-1-401, Fukuda, Yamato-shi, Kanagawa-ken, JP Nationality: JP MATSUNAGA, KOZO, 7-8-1-202, Kamitsuruma, Sagamihara, Sagamihara-shi, Kanagawa-ken, JP Nationality: JP
Language: EN (14 pages, 7 drawings)
Application: US 2002248116 A 20021219 (Local application)
Priority: JP 2001395303 A 20011226
Original IPC: H04Q-7/24(A)
Current IPC: H04L-12/28(R,I,M,EP,20060101,20051008,A) H04L-12/28 (R,I,M,EP,20060101,20051008,C) H04L-29/06(R,I,M,EP,20060101,20051008,A) H04L-29/06 (R,I,M,EP,20060101,20051008,C)
Original US Class (secondary): 370328 370338
Original Abstract: Abstract of the DisclosureIn a network security system, clients search for neighbor access points (APs) in order to establish wireless connections to a LAN. As a result of the search, each of the clients dispatches a list of access points obtained to a controller. The controller detects non-registered access points by comparing a list of previously registered access points with the lists dispatched by the clients.
Claim: What is Claimed is: 1.Apparatus comprising: * **1.** a client permitted to establish a wireless connection to a ne twork through an access point; and * a controller permitted to receive data dispatched by said client, thr ough said network, * wherein said client scans electromagnetic waves within bands permitte d to be used for wireless communication, and dispatches to said contr oller identification information on access points detected as a resul t of the scan, and * said controller stores said identification information on access poin ts permitted to access said network, and on the basis of the

identifi cation information on the permitted access points and said identifica tion information dispatched by said client, extracts non-registered a ccess points that are not registered as permitted access points.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－198571
（P2003－198571A）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/28	３１０	Ｈ０４Ｌ　12/28	３１０	５Ｋ０３３
Ｇ０６Ｆ　13/00	５１０	Ｇ０６Ｆ　13/00	５１０Ａ	５Ｋ０６７
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　有　　請求項の数18　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－395303(P2001－395303)

(22)出願日　平成13年12月26日(2001.12.26)

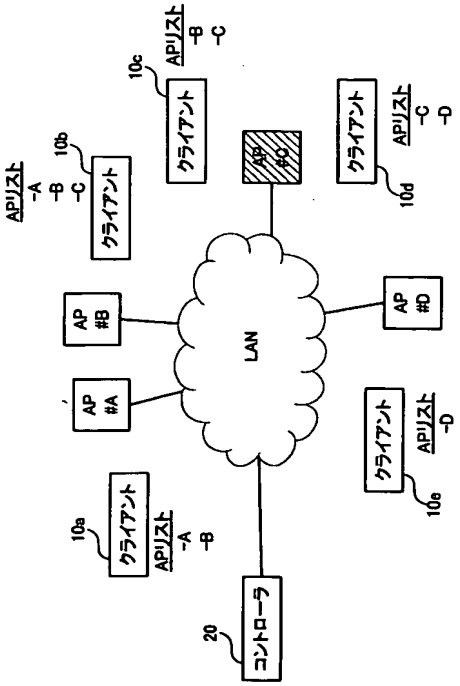
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

(74)代理人　100086243
弁理士　坂口　博　（外３名）

最終頁に続く

(54)【発明の名称】　ネットワークセキュリティシステム、コンピュータ装置、アクセスポイントの認識処理方法、アクセスポイントのチェック方法、プログラム、記憶媒体および無線ＬＡＮ用デバイス

(57)【要約】
【課題】　無線ＬＡＮにおいてセキュリティを強化することができるシステムを提供する。
【解決手段】　ネットワークセキュリティシステムでは、クライアント１０ａ～ｅは無線を通じてＬＡＮに接続するため、近くのアクセスポイント（ＡＰ）をサーチする。サーチの結果、得られたアクセスポイントのリストをコントローラ２０へ送出する。コントローラ２０では、予め登録されたアクセスポイントのリストと、各クライアント１０ａ～ｅから送出されたリストと、を比較し、未登録のアクセスポイントを検出する。



【特許請求の範囲】

【請求項１】　アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、

前記ネットワークを介して前記クライアントから送出されたデータの受信が可能なコントローラと、を備え、

前記クライアントは、無線通信可能な帯域の電波をスキャンし、その結果検出されたアクセスポイントの識別情報を前記コントローラへ送出し、

前記コントローラは、前記ネットワークに対してアクセスが許可された許可アクセスポイントの識別情報を格納し、当該許可アクセスポイントの当該識別情報と前記クライアントから送出された前記識別情報とに基づき、検出された前記アクセスポイントのうち、当該許可アクセスポイントとして登録されていない未登録アクセスポイントを抽出することを特徴とするネットワークセキュリティシステム。

【請求項２】　前記クライアントは、前記無線接続には使用しない前記アクセスポイントの前記識別情報を前記コントローラに送出することを特徴とした請求項１記載のネットワークセキュリティシステム。

【請求項３】　前記クライアントは、前記アクセスポイントから受信した信号の強度を前記コントローラへ送出し、

前記コントローラは、前記強度に基づき、前記未登録アクセスポイントの設置エリアを推定することを特徴とする請求項１記載のネットワークセキュリティシステム。

【請求項４】　ネットワークに接続されたアクセスポイントと無線通信が可能なコンピュータ装置であって、

アクセスポイントから発生する電波に基づいて、当該アクセスポイントの識別情報を認識する認識部と、

前記認識部で認識された前記識別情報を記憶する記憶部と、

前記記憶部に記憶された前記識別情報を前記ネットワークを介して送出する送出部と、

を備えたことを特徴とするコンピュータ装置。

【請求項５】　前記送出部は、所定時間毎に、または前記ネットワークを介した要求に応じて、前記識別情報を送出することを特徴とする請求項４記載のコンピュータ装置。

【請求項６】　アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、当該ネットワークを介してデータの送受信が可能なコントローラであって、

前記ネットワークに対してアクセスが許可された許可アクセスポイントの許可リストを格納する格納部と、

前記クライアントにより無線通信可能な帯域の電波がスキャンされることにより認識された認識アクセスポイントの認識リストを収集する収集部と、

前記許可リストおよび前記認識リストに基づき、前記認識リストに含まれる前記認識アクセスポイントのうち、

前記許可リストに含まれていない未登録アクセスポイントを抽出する抽出部と、

を備えたことを特徴とするコンピュータ装置。

【請求項７】　前記ネットワークにおける前記許可アクセスポイントの設置位置情報を格納する設置位置情報格納部と、

前記認識アクセスポイントから発生した信号の強度を収集する信号収集部と、

前記強度と前記設置位置情報に基づき、前記未登録アクセスポイントの設置位置を算出する算出部と、

をさらに備えたことを特徴とする請求項６記載のコンピュータ装置。

【請求項８】　ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置におけるアクセスポイントの認識処理方法であって、

無線通信可能な帯域の電波をスキャンするステップと、

前記スキャンによって検出されたアクセスポイントのリストを取得するステップと、

取得した前記リストを前記ネットワークを介して送出するステップと、

を有することを特徴とするアクセスポイントの認識処理方法。

【請求項９】　前記アクセスポイントから発生する信号の強度を取得するステップと、

前記強度を前記ネットワークを介して送出するステップと、

をさらに有することを特徴とする請求項８記載のアクセスポイントの認識処理方法。

【請求項１０】　コンピュータ装置を無線によりネットワークへ繋ぐため、当該ネットワークに接続されるアクセスポイントをチェックする方法であって、

前記ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得するステップと、

前記コンピュータ装置により認識されたアクセスポイントの検出リストを取得するステップと、

前記許可リストと前記検出リストを比較し、当該検出リストに含まれる前記アクセスポイントのうち、当該許可リストに含まれない未登録アクセスポイントを認識するステップと、

を有することを特徴とするアクセスポイントのチェック方法。

【請求項１１】　前記許可リストに含まれる前記アクセスポイントの設置箇所を登録するステップと、

前記コンピュータ装置のスキャンによって検出された前記アクセスポイントからの信号の強度を取得するステップと、

前記強度に基づき、前記未登録アクセスポイントの設置箇所を算出するステップと、

をさらに有することを特徴とする請求項１０記載のアクセスポイントのチェック方法。

【請求項１２】　ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置に実行させるためのプログラムであって、
無線通信可能な帯域の電波をスキャンする手順と、
前記スキャンによって検出されたアクセスポイントのリストを記録する手順と、
前記リストを前記ネットワークを介して送出する手順と、
を備えたことを特徴とするコンピュータ装置に実行させるためのプログラム。
【請求項１３】　前記アクセスポイントから発生する振動の強度を取得する手順と、
前記強度を前記ネットワークを介して送出する手順と、
をさらに備えたことを特徴とする請求項１２記載のコンピュータ装置に実行させるためのプログラム。
【請求項１４】　コンピュータ装置を無線によりネットワークへ繋ぐため、当該ネットワークに接続されるアクセスポイントをチェックするプログラムであって、
前記ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得する手順と、
前記コンピュータ装置により認識されたアクセスポイントの検出リストを取得する手順と、
前記許可リストと前記検出リストを比較し、当該検出リストに含まれる前記アクセスポイントのうち、当該許可リストに含まれない未登録アクセスポイントを認識する手順と、
を有することを特徴とするコンピュータ装置に実行させるためのプログラム。
【請求項１５】　前記許可リストに含まれる前記アクセスポイントの設置箇所を登録する手順と、
前記コンピュータ装置のスキャンによって検出された前記アクセスポイントからの信号の強度を取得する手順と、
前記強度に基づき、前記未登録アクセスポイントの設置箇所を算出する手順と、
をさらに有することを特徴とする請求項１４記載のコンピュータ装置に実行させるためのプログラム。
【請求項１６】　ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置に実行させるためのプログラムを、当該コンピュータ装置が読み取り可能に記憶した記憶媒体であって、
無線通信可能な帯域の電波をスキャンする機能と、
前記スキャンによって検出されたアクセスポイントのリストを記録する機能と、
前記リストを前記ネットワークを介して送出する機能と、
を前記コンピュータ装置に実現させるプログラムを記憶したことを特徴とする記憶媒体。
【請求項１７】　コンピュータ装置を無線によりネットワークへ繋ぐため、当該ネットワークに接続されるアクセスポイントをチェックさせるためのプログラムを、当該コンピュータ装置が読み取り可能に記憶した記憶媒体であって、
前記ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得する機能と、
前記コンピュータ装置により認識されたアクセスポイントの検出リストを取得する機能と、
前記許可リストと前記検出リストを比較し、当該検出リストに含まれる前記アクセスポイントのうち、当該許可リストに含まれない未登録アクセスポイントを認識する機能と、
を前記コンピュータ装置に実現させるプログラムを記憶したことを特徴とする記憶媒体。
【請求項１８】　無線ＬＡＮを介してネットワークとデータの送受信を行うため、コンピュータ装置に接続可能な無線ＬＡＮ用デバイスであって、
アクセスポイントをサーチするためのスキャンを行うスキャン部と、
前記スキャン部によって検出された前記アクセスポイントのＩＤを記録するＩＤ記録部と、
前記記録部に記録された前記ＩＤを前記ネットワークへ送出する送出部と、
を備えたことを特徴とする無線ＬＡＮ用デバイス。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークセキュリティシステム等に関し、より詳しくは不正に接続されたアクセスポイントを検出できるネットワークセキュリティシステム等に関する。
【０００２】
【従来の技術】従来、職場や家庭内等、様々な箇所でコンピュータ装置が広く使用されている。汎用されているコンピュータ装置の種類としては、机等の所定の場所にほぼ固定されて使用されるデスクトップ型ＰＣ(Personal Computer)や、可搬性を考慮して比較的小型に設計されたノートブック型ＰＣ、ＰＤＡ(Personal Digital Assistant)等を挙げることができる。これらコンピュータ装置においては、ネットワークを介して外部とのデータの送受信が行われているが、特に近年では無線ＬＡＮモジュールを用いてデータの送受信が無線により行われている。この無線ＬＡＮモジュールが導入されていると、コンピュータ装置はネットワークに接続された無線基地局（以下、アクセスポイントという）とデータの送受信ができる限り、移動先においても外部とのデータの送受信を簡単に行うことができる。
【０００３】ところで、このようなアクセスポイントとのデータの送受信においては、接続を許可されていないコンピュータ装置がネットワークに不正に接続し、データを盗むことがしばしば起きている。そこで、ネットワークにおいてこのような不正な接続を防ぐために様々な

処理が行われており、例えば、ＷＥＰ（Wired Equivalent Privacy）と呼ばれる手法では、６４または１２８bitのキーに基づいて、データを暗号化し、エラーや改ざんの有無をチェックすることで不正な接続を防止する。しかし、ＷＥＰでは、キーを不正に入手されてしまった場合、暗号化されたデータは容易に復号化されてしまう。一方、ＭＡＣ（Media Access Control） Ａｄｄｒｅｓｓ Ｆｉｌｔｅｒｉｎｇと呼ばれる手法では、予めアクセスを許可されたコンピュータ装置のＭＡＣアドレス以外のＭＡＣアドレスを有するコンピュータ装置のアクセスを禁止している。しかし、ＭＡＣアドレスを偽造することは比較的簡単にできてしまうので、許可されていないコンピュータ装置の不正なアクセスを完全に防止する機能を期待するのは難しい。

【０００４】そこで、最近では複数の手法を組み入れた方法が採用されている。例えば、ユーザＩＤとパスワードにより所定のユーザの接続を管理し、ＭＡＣ（Media Access Control） Ａｄｄｒｅｓｓ Ｆｉｌｔｅｒｉｎｇにより所定のコンピュータ装置の接続を管理し、さらに802.1xと呼ばれる手法によりデータの暗号化を行う。802.1xとは、コンピュータ装置とアクセスポイントとのセッション毎に、上記のＷＥＰキーを動的に生成し、そのＷＥＰキーを利用して認証を行う。すなわちこの方法では、セッション毎にキーが変わるので、万が一キーが盗まれても、次回のセッションにおいてはそのキーは無効となる。

【０００５】

【発明が解決しようとする課題】しかしながら、不正なアクセスポイントがネットワークに接続されることで、以上述べた方法も無効になってしまう場合がある。一般にＷＥＰキーは、コンピュータ装置またはアクセスポイントのメモリ内に保存され、ＷＥＰキーの認証はアクセスポイント側から一方向に行われる。そのため、アクセスポイント側はコンピュータ装置を使用するユーザを認証するが、ユーザ側がアクセスポイントを認証することは殆ど不可能である。したがって、不正にアクセスポイントが設置された場合、そこからデータを不正に入手されたり、正当なユーザのクライアントが乗っ取られたりしてしまう可能性がある。

【０００６】また、ＷＥＰキーの認証を両方向、すなわちコンピュータ装置側とアクセスポイント側が相互に行うことも不可能ではないが、サーバやクライアントとは別の認証サーバをネットワーク上に設置しなければならず、また認証の設定や不正アクセスの管理に大変手間がかかる。

【０００７】本発明は、上記のような技術的課題に基づいてなされたもので、無線通信を行うネットワークにおいてセキュリティを高めることが可能なネットワークセキュリティシステム等を提供することを主たる目的とする。

【０００８】

【課題を解決するための手段】かかる目的のもと、本発明のネットワークセキュリティシステムは、アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、ネットワークを介してクライアントから送出されたデータの受信が可能なコントローラとを備え、クライアントは、無線通信可能な帯域の電波をスキャンし、その結果検出されたアクセスポイントの識別情報をコントローラへ送出し、コントローラは、ネットワークに対してアクセスが許可された許可アクセスポイントの識別情報を格納し、許可アクセスポイントの識別情報とクライアントから送出された識別情報とに基づき、検出されたアクセスポイントのうち、許可アクセスポイントとして登録されていない未登録アクセスポイントを抽出することを特徴とするものである。このネットワークセキュリティシステムでは、予め許可されたアクセスポイントと、クライアントが検出したアクセスポイントとを比較することにより、登録されていないアクセスポイントを見つけ出すことが可能である。

【０００９】このネットワークセキュリティシステムでは、クライアントは、無線接続には使用しないアクセスポイントの識別情報をコントローラに送出することが可能である。また、クライアントは、アクセスポイントから受信した信号の強度をコントローラへ送出し、コントローラは、強度に基づき、未登録アクセスポイントの設置エリアを推定することができる。

【００１０】また、本発明はコンピュータ装置として捉えることもできる。このコンピュータ装置は、ネットワークに接続されたアクセスポイントと無線通信が可能なコンピュータ装置であって、アクセスポイントから発生する電波に基づいて、アクセスポイントの識別情報を認識する認識部と、認識部で認識された識別情報を記憶する記憶部と、記憶部に記憶された識別情報を、ネットワークを介して送出する送出部と、を備えたことを特徴とするものである。ここで、送出部は、所定時間毎に、またはネットワークを介した要求に応じて、識別情報を送出することができる。

【００１１】さらに本発明のコンピュータ装置は、アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、ネットワークを介してデータの送受信が可能なコントローラであって、ネットワークに対してアクセスが許可された許可アクセスポイントの許可リストを格納する格納部と、クライアントにより無線通信可能な帯域の電波がスキャンされることにより認識された認識アクセスポイントの認識リストを収集する収集部と、許可リストおよび認識リストに基づき、認識リストに含まれる認識アクセスポイントのうち、許可リストに含まれていない未登録アクセスポイントを抽出する抽出部と、を備えたことを特徴とするものである。

【００１２】このコンピュータ装置は、ネットワークに

おける許可アクセスポイントの設置位置情報を格納する設置位置情報格納部と、認識アクセスポイントから発生した信号の強度を収集する信号収集部と、強度と設置位置情報に基づき、未登録アクセスポイントの設置位置を算出する算出部と、をさらに備えることができる。

【００１３】その他、本発明はアクセスポイントの認識処理方法として捉えることができる。このアクセスポイントの認識処理方法は、ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置におけるアクセスポイントの認識処理方法であって、無線通信可能な帯域の電波をスキャンするステップと、スキャンによって検出されたアクセスポイントのリストを取得するステップと、取得したリストをネットワークを介して送出するステップと、アクセスポイントから発生する信号の強度を取得するステップと、強度をネットワークを介して送出するステップと、を有することを特徴とする方法である。

【００１４】また、本発明はアクセスポイントのチェック方法として捉えることができる。このアクセスポイントのチェック方法は、コンピュータ装置を無線によりネットワークへ繋ぐため、ネットワークに接続されるアクセスポイントをチェックする方法であって、ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得するステップと、コンピュータ装置により認識されたアクセスポイントの検出リストを取得するステップと、許可リストと検出リストを比較し、検出リストに含まれるアクセスポイントのうち、許可リストに含まれない未登録アクセスポイントを認識するステップと、許可リストに含まれるアクセスポイントの設置箇所を登録するステップと、コンピュータ装置のスキャンによって検出されたアクセスポイントからの信号の強度を取得するステップと、強度に基づき、未登録アクセスポイントの設置箇所を算出するステップと、を有することを特徴とする方法である。

【００１５】さらに本発明はコンピュータに実行させるプログラムとして捉えることができる。このプログラムは、ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置に実行させるためのプログラムであって、無線通信可能な帯域の電波をスキャンする手順と、スキャンによって検出されたアクセスポイントのリストを記録する手順と、リストをネットワークを介して送出する手順と、アクセスポイントから発生する振動の強度を取得する手順と、強度をネットワークを介して送出する手順と、を備えたことを特徴とするプログラムである。

【００１６】また本発明のプログラムは、コンピュータ装置を無線によりネットワークへ繋ぐため、ネットワークに接続されるアクセスポイントをチェックするプログラムであって、ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得する手順と、コンピュータ装置により認識されたアクセスポイントの検出リストを取得する手順と、許可リストと検出リストを比較し、検出リストに含まれるアクセスポイントのうち、許可リストに含まれない未登録アクセスポイントを認識する手順と、許可リストに含まれるアクセスポイントの設置箇所を登録する手順と、コンピュータ装置のスキャンによって検出されたアクセスポイントからの信号の強度を取得する手順と、強度に基づき、未登録アクセスポイントの設置箇所を算出する手順と、を有することを特徴とするプログラムである。

【００１７】その他、本発明は、プログラムを記憶した記憶媒体や、コンピュータ装置に接続可能な無線ＬＡＮ用デバイスを提供することもできる。

【００１８】

【発明の実施の形態】以下、添付図面に示す実施の形態に基づいて本発明を詳細に説明する。図１は、本実施の形態における無線通信を利用したＬＡＮ（Local Area Network）システム（ネットワークセキュリティシステム）を説明するための構成図である。図１に示すＬＡＮシステムでは、ユーザの使用する端末であるクライアント（コンピュータ装置）１０ａ、１０ｂ、１０ｃ、１０ｄ、１０ｅ（以下、１０ａ～ｅと略する場合がある）と、システム管理者の使用する端末であるコントローラ（コンピュータ装置）２０と、アクセスポイント（以下、ＡＰと言う）ＡＰ＃Ａ、ＡＰ＃Ｂ、ＡＰ＃Ｃ、ＡＰ＃Ｄ（以下、ＡＰ＃Ａ～Ｄと略する場合がある）が備えられている。クライアント１０ａ～ｅは、ＡＰ＃Ａ～Ｄを介してネットワークに接続可能とされている。また、コントローラ２０は有線によってネットワークに接続されている。但し、コントローラ２０もＡＰ＃Ａ～Ｄを介してネットワークに接続されるものであってもよい。

【００１９】図２は、クライアント１０ａ～ｅの構成を示した図である。図２に示すクライアント１０ａ～ｅは、ＣＰＵ等の演算処理部（認識部）１１と、メモリ１２と、ＨＤＤ（Hard Disk Drive、記憶部）１３と、ユーザからの入力を受け付け、ユーザに対してデータを出力する入出力部１４と、ネットワークを介して外部とデータの送受信を行う送受信部（認識部）１５を備えている。さらに送受信部１５は、ＡＰをサーチする機能を有するＡＰサーチ部１６と、取得したＡＰリストをコントローラ２０へ送出する機能を有するＡＰリスト送出部１７と、アンテナ１８とを備えている。また、ＨＤＤ１３は、取得したＡＰリストを保存するＡＰリスト記憶部１９を備えている。

【００２０】なお、図示していないが、クライアント１０ａ～ｅが有する送受信部１５は、アンテナ１８に連絡しているパワー増幅器、ＲＦ／ＩＦコンバータ・シンセサイザ、Ｉ／Ｑモジュレータ・デモジュレータ、ベースバンドプロセッサ、電波の送受信をコントロールするメディア・アクセス・コントローラ等を備えている。これ

らはＬＡＮカードまたはＬＡＮボードとして、例えばＩＥＥＥ８０２．１１の規格に準拠したものであり、例えば２．４ＧＨｚ帯の電波を使うもの、５ＧＨｚ帯の電波を使うもの、赤外線を使うもの等を使用することができる。

【００２１】図３は、コントローラ２０の構成を示した図である。図３に示すコントローラ２０は、ＣＰＵ等の演算処理部２１と、メモリ２２と、ＨＤＤ２３と、ユーザからの入力を受け付け、ユーザに対してデータを出力する入出力部２４と、ネットワークを介して外部とデータの送受信を行う送受信部２５を備えている。さらに、演算処理部２１は、取得したＡＰリストと登録されているＡＰリストを比較する機能を有するＡＰリスト比較処理部（抽出部）２６を備えている。また、ＨＤＤ２３は、接続を許可されたＡＰのリストを登録したＡＰリスト登録部（格納部）２７を備えている。そして、送受信部２５は、クライアント１０ａ～ｅから送出されたＡＰリストを受信する機能を有するＡＰリスト受信部（収集部）２８を備えている。

【００２２】なお、上記のクライアント１０ａ～ｅやコントローラ２０は、ユーザが使用するコンピュータ装置であって、例えばノートブック型ＰＣ（Personal Computer）や、デスクトップ型ＰＣや、ＰＤＡ等であり、これらのコンピュータ装置が備えるその他の部材を有することができる。また、クライアント１０ａ～ｅおよびコントローラ２０は互いに同じコンピュータ装置であってもよく、または異なるコンピュータ装置であってもよい。

【００２３】通常、無線ＬＡＮにより外部とのデータ送受信を行う場合、クライアント１０ａ～ｅの送受信部１５はデータの送受信を確実に行うために、定期的にＡＰの探索を行う。ＡＰの探索では、まず所定周波数の電波でスキャンを行い、通信を確立できるＡＰを見つける。そして、そのＡＰとのデータ送受信ができることがＡＰとクライアント１０ａ～ｅとの間で確認が取れた後、データの送受信を開始する。本実施の形態におけるＬＡＮシステムでは、探索されたＡＰの情報を基に、不正なＡＰがネットワーク内に存在することを検出することができる。以下、不正なＡＰを検出する方法を具体的に説明する。

【００２４】図４は、クライアント１０ａ～ｅにおける処理の流れを示す図である。ここで、クライアント１０ａ～ｅにおける処理は、クライアント１０ａ～ｅにインストールされたコンピュータ用のプログラムを実行することによって行われる。なお、クライアント１０ａ～ｅは同じプログラムに基づいて処理を行うので、クライアント１０ａを例に挙げて説明する。

【００２５】まず、ＨＤＤ１３のＡＰリスト記憶部１９に記憶されているＡＰリスト（以前にＡＰのサーチが行われている場合、そのとき得られたＡＰリスト）を消去する（ステップＳ１０１）。続けて、接続するＡＰを探すために電波をスキャンしてクライアント１０ａとへ電波を到達させることができるＡＰをサーチして見つける（ステップＳ１０３）。ここで、ＡＰのスキャンおよびサーチについて詳細を説明する。

【００２６】図５は、送受信部１５のＡＰサーチ部１６によるスキャンおよびＡＰのサーチについての処理の流れを説明する図である。まず、電波のチャンネルナンバー（以下、チャンネルＮｏ．）を１に設定する（ステップＳ１１１）。この設定において、クライアント１０ａは、アンテナ１８を介してビーコンを受信できたか否かを判断する（ステップＳ１１３）。ビーコンを受信できなかったと判断した場合、後述のステップＳ１１７の処理を行う。一方、ビーコンを受信したと判断した場合、通信相手を特定するための識別番号であるＳＳＩＤ（Service Set Identification）とビーコンの信号強度をＡＰリスト記憶部１９のＡＰリストに追加する（ステップＳ１１５）。例えばクライアント１０ａの場合、図１に示すように、クライアント１０ａの近辺に位置するＡＰであるＡＰ＃ＡおよびＡＰ＃ＢがＡＰリスト記憶部１９に記憶される。

【００２７】続いて、スキャンする電波のチャンネルＮｏ．を増加させる（ステップＳ１１７）。そして、増加させたチャンネルＮｏ．が、送受信部１５が受信できる最大チャンネルＮｏ．より大きいか否かを判断する（ステップＳ１１９）。チャンネルＮｏ．が最大チャンネルＮｏ．より大きくないと判断した場合、ステップＳ１１３へ戻って同様の処理を行う。一方、チャンネルＮｏ．が最大チャンネルＮｏ．大きいと判断した場合、スキャンおよびＡＰのサーチの処理を終了する。

【００２８】以上のようにして得られた、ＡＰリストを、図４に示すように、送受信部１５のＡＰリスト送出部１７によりコントローラ２０へ送出する（ステップＳ１０５）。そして、所定の待機時間（ｔ）が経過するのを待機し（ステップＳ１０７）、待機が終了すると、再度ステップＳ１０１へ戻って処理を開始する。このように、スキャンおよびＡＰのサーチ処理においては、クライアント１０ａ～ｅにおいて、それぞれ電波の受信ができるＡＰ、すなわち認識できるＡＰのチャンネルと、そのＡＰからの信号強度の情報を受信する。そして、各クライアント１０ａ～ｅは、図１に示すようにＡＰリストを取得する。

【００２９】図６は、コントローラ２０における処理の流れを説明する図である。ここで、コントローラ２０における処理は、コントローラ２０にインストールされたコンピュータ用のプログラムによって行われる。まず、各クライアント１０ａ～ｅから送信されたＡＰリストを送受信部２５のＡＰリスト受信部２８にて受信する（ステップＳ２０１）。ここで受信したリストは、メモリ２２上に一時的に記憶される。そして、待機時間（ｔ）が

経過したか否かを判断する（ステップＳ２０３）。この待機時間（ｔ）は、複数のクライアント１０ａ～ｅから時を同じくせず送信されてくるＡＰリストを、できるだけ多くのクライアント１０ａ～ｅから受信するためである。待機時間（ｔ）は、例えば１時間おきに設定することができる。ステップＳ２０３において、待機時間（ｔ）が経過していないと判断すると、ステップＳ２０３の処理が再度行われる。

【００３０】一方、ステップＳ２０３において待機時間（ｔ）が経過していると判断すると、受信したＡＰリストの集合体である収集ＡＰリストと、ＨＤＤ２３のＡＰリスト登録部２７に登録されている管理用ＡＰリストと、の比較をＡＰリスト比較処理部２６により行う（ステップＳ２０５）。管理用ＡＰリストは、ネットワークへのアクセスを許可された真正なるアクセスポイントのリストであって、管理者ＡＰリスト中のアクセスポイントは、ネットワークに接続されているアクセスポイントと一致することが確認されているものである。管理用ＡＰリストは、例えばシステム管理者により作成される。その他、真正なるアクセスポイントは、各クライアント１０ａ～ｅ等より認証の要求がなされたアクセスポイントであって、システム管理者により真正なアクセスポイントであると認証されたものであってもよい。

【００３１】ここで、図７(a)に各クライアント１０ａ～ｅから受信したＡＰリストの一例を示し、(b)に収集ＡＰリストとＡＰリスト登録部２７に登録されている管理用ＡＰリストのデータの一例を示す。図７(a)に示すように、各クライアント１０ａ～ｅから収集したＡＰリストから、実際にネットワークに接続しているＡＰのデータを、収集ＡＰリストとして取得する。そして、収集ＡＰリストと登録ＡＰリストとを比較して、収集ＡＰリストのうち、登録ＡＰリストに登録されていないＡＰ、すなわち不正ＡＰを抽出する。図７(b)に示す場合では、登録されていないＡＰとしてＡＰ＃Ｃが抽出される。

【００３２】続けて、不正ＡＰの検出処理に基づき、不正ＡＰがあるか否かを判断する（ステップＳ２０７）。不正ＡＰは無いと判断した場合、ステップＳ２０１へ戻って処理を続ける。不正ＡＰがあると判断した場合、コントローラ２０のユーザに対して入出力部２４を介して警告を発する（ステップＳ２０９）。その後、ステップＳ２０１に戻って処理を続ける。

【００３３】ここで、ステップＳ２０９における警告では、不正ＡＰの存在と共に、不正ＡＰの存在箇所を推定して提示することができる。例えば、コントローラ２０のＨＤＤ２３にネットワークに接続可能である正規に登録されたＡＰの設置箇所を示した構成図を記録し、クライアント１０ａ～ｅから受信したＡＰリストには、それぞれのＡＰに対する信号強度を含ませる。この場合、正規のＡＰの設置箇所から、どの程度離れた位置にそのクライアント１０ａ～ｅが存在するかを認識することができ、さらにクライアント１０ａ～ｅによって認識された不正ＡＰについての信号強度を基に、不正ＡＰの大よその位置を掴むことが可能となる。このようにしてコントローラ２０を介して警告と不正ＡＰの位置情報を得ることで、その情報を基に不正ＡＰを探し出し、その不正ＡＰの撤去を行うことが可能となる。

【００３４】以上のように、本実施の形態では、無線ＬＡＮネットワークに接続しているクライアント１０ａ～ｅにより、クライアント１０ａ～ｅが認識できるＡＰのデータが送出され、そのリストに載ったＡＰを予め登録されたＡＰと比較することで、不正なＡＰを簡単に検出することができる。従来の無線ＬＡＮネットワークでは、クライアント１０ａ～ｅは使用できるＡＰを認識するためサーチを行い、クライアント１０ａ～ｅに電波が届くＡＰの認識を行っていたが、データの送受信を行うＡＰを特定するだけで処理を終了していた。そこで本実施の形態では、クライアント１０ａ～ｅが得た情報を収集して利用することで、簡単に且つ確実に不正ＡＰの検出を可能とした。

【００３５】また、本実施の形態では、ＡＰリストを取得する処理は、クライアント１０ａ～ｅとして通常に使用するコンピュータ装置に所定のプログラムをインストールするだけで、実行することができる。また、コントローラ２０に対しても同様に所定のプログラムをインストールして正規なＡＰを登録するだけで、不正ＡＰの検出を行うことができる。よって、本実施の形態では、低コストで簡単に不正ＡＰの検出を行うことが可能である。

【００３６】なお、上記実施の形態において、コントローラ２０の代わりに、クライアント１０ａ～ｅのいずれかにコントローラ２０の機能を備えさせることが可能である。その場合、コントローラ２０に導入するプログラムを、クライアント１０ａ～ｅのいずれかにインストールすればよい。さらに、各クライアント１０ａ～ｅのＨＤＤ１３に登録された正規のＡＰリストを記憶させ、各クライアント１０ａ～ｅにおいて不正ＡＰを検出するものであってもよい。

【００３７】また、上記実施の形態においては、各クライアント１０ａ～ｅからコントローラ２０へ対して自動的にＡＰリストが送出されているが、本実施の形態はこれに限定されない。例えば、コントローラ２０側から各クライアント１０ａ～ｅにアクセスして要求することで、ＡＰリストを取得するものであってもよい。この場合、クライアント１０ａ～ｅが検出するＡＰリストの取得は定期的に行うこともできるが、システム管理者が取得を希望する時、例えば１日に２～３回任意に取得することも可能である。

【００３８】さらに、上記実施の形態においては、クライアント１０ａ～ｅがＡＰリストを取得する処理のタイ

ミングを決める間隔を待機時間（ｔ）とし、コントローラ２０がクライアント１０ａ～ｅから受信したＡＰリストを比較処理するタイミングを決める間隔を同じく待機時間（ｔ）としているが、本実施の形態はこれに限定されない。例えば、クライアント１０ａ～ｅが頻繁に移動して使用されることを考慮した場合、クライアント１０ａ～ｅはより接続しやすいＡＰを頻繁に探す、即ち頻繁にＡＰリストを入手する。それに対してこのＡＰリストはコントローラ２０に対して頻繁には送出せず、例えば数時間おきに送出するものであってもよい。また、頻繁に送出するものであっても、コントローラ２０における待機時間（ｔ）を長く設定することで、不正ＡＰの検出の回数を制御することもできる。

【００３９】また、上記実施の形態においては、検出された不正ＡＰは位置を検出されて撤去されているが、本実施の形態はこれに限定されない。例えば、その不正ＡＰが接続しているルータを操作することで、不正ＡＰとのデータの送受信を禁止させるものであってもよい。また、不正ＡＰが存在することのみ警告を発し、不正ＡＰの位置の検出はコントローラ２０以外で行われるものであってもよい。

【００４０】その他、上記実施の形態においては、導入されたプログラムによってクライアント１０ａ～ｅとコントローラ２０における処理を実行しているが、本実施の形態はこれに限定されない。例えば、プログラムを導入する代わりに、クライアント１０ａ～ｅに接続される無線通信用デバイス（無線ＬＡＮ用ＰＣカードやボード等）に、取得したＡＰリストを定期的にコントローラ２０に対して送信する機能を持たせることもできる。この場合、無線通信用デバイスをクライアント１０ａ～ｅに接続するだけで、不正ＡＰを検出するためのクライアント１０ａ～ｅとしての機能を果たすことが可能となる。また、コントローラ２０についても同様に、ネットワークに接続するためのデバイスにコントローラ２０としての機能を持たせることができる。

【００４１】なお、本実施の形態で示したような処理を行うためのプログラムは、以下のような記憶媒体、プログラム伝送装置の形態とすることもできる。すなわち、記憶媒体としては、コンピュータ装置に実行させるプログラムを、ＣＤ－ＲＯＭ、ＤＶＤ、メモリ、ハードディスク等の記憶媒体に、コンピュータ装置が読み取り可能となるように記憶させれば良い。また、プログラム伝送装置としては、上記したようなプログラムを記憶させたＣＤ－ＲＯＭ、ＤＶＤ、メモリ、ハードディスク等の記憶手段と、この記憶手段から当該プログラムを読み出し、当該プログラムを実行する装置側に、コネクタ、あるいはインターネットやＬＡＮ等のネットワークを介して当該プログラムを伝送する伝送手段とを備える構成とすれば良い。これ以外にも、本発明の主旨を逸脱しない限り、上記実施の形態で挙げた構成を取捨選択したり、他の構成に適宜変更することが可能である。

【００４２】

【発明の効果】このように本発明によれば、無線ネットワークエリア内に設けられた不正なアクセスポイント（ＡＰ）を簡単に検出することができる。

【図面の簡単な説明】

【図１】　本実施の形態におけるＬＡＮシステムを説明するための構成図である。

【図２】　クライアントの構成を示した図である。

【図３】　コントローラの構成を示した図である。

【図４】　クライアントにおける処理の流れを示す図である。

【図５】　クライアントのＡＰサーチ部によるスキャンおよびＡＰのサーチについての処理の流れを説明する図である。

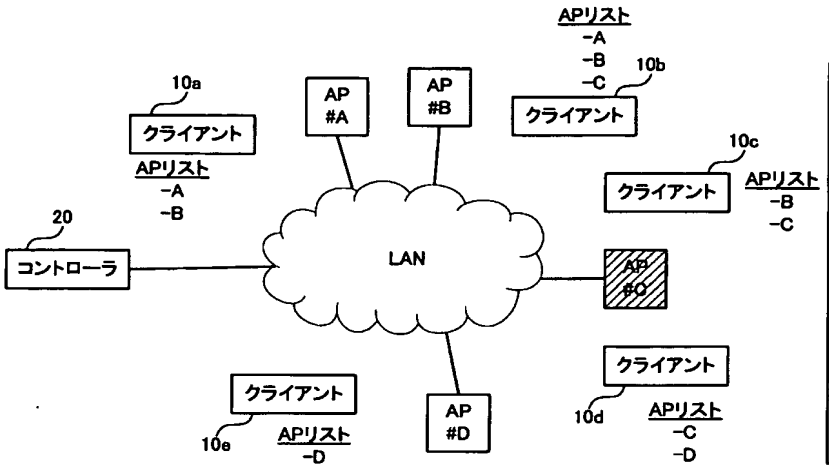
【図６】　コントローラにおける処理の流れを説明する図である。

【図７】　(a)は各クライアント１０ａ～ｅから受信したＡＰリストの一例を示す図であり、(b)は収集ＡＰリストとＡＰリスト登録部に登録されている管理用ＡＰリストのデータの一例を示す図である。

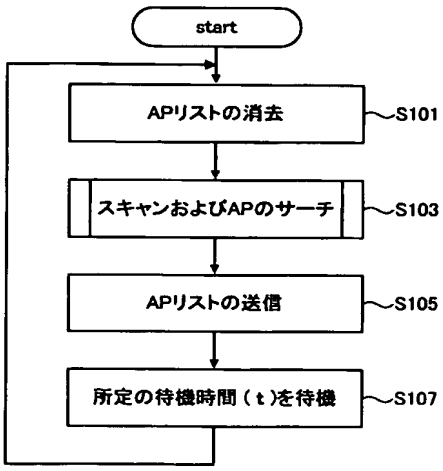
【符号の説明】

１０ａ、１０ｂ、１０ｃ、１０ｄ、１０ｅ…クライアント（コンピュータ装置）、１１…演算処理部（認識部）、１３…ＨＤＤ（記憶部）、１５…送受信部（認識部）、１６…ＡＰサーチ部、１７…ＡＰリスト送出部、１８…アンテナ、１９…ＡＰリスト記憶部、２０…コントローラ（コンピュータ装置）、２１…演算処理部、２３…ＨＤＤ、２５…送受信部、２６…ＡＰリスト比較処理部（抽出部）、２７…ＡＰリスト登録部（格納部）、２８…ＡＰリスト受信部（収集部）、ＡＰ＃Ａ、ＡＰ＃Ｂ、ＡＰ＃Ｃ、ＡＰ＃Ｄ…アクセスポイント

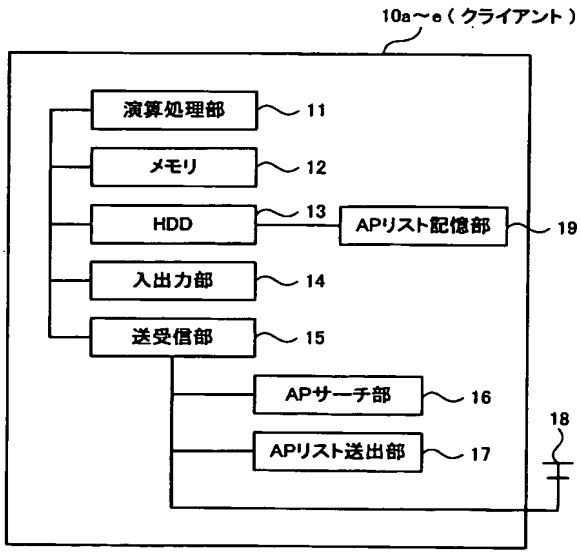
【図１】


APリスト
-A
-B
-C
10a
クライアント
APリスト
-A
-B
AP
#A
AP
#B
10b
クライアント
10c
クライアント
APリスト
-B
-C
20
コントローラ
LAN
AP
#C
クライアント
10e
APリスト
-D
AP
#D
クライアント
10d
APリスト
-C
-D

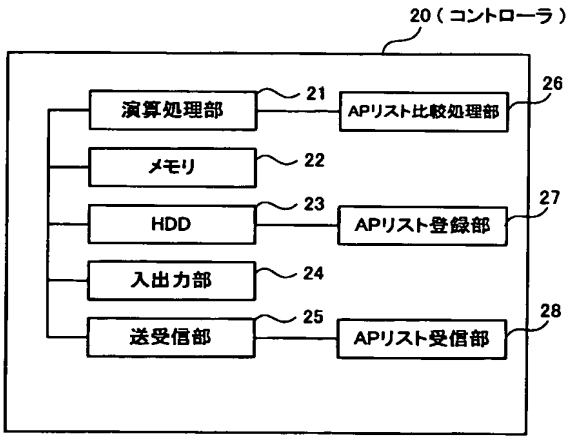
【図４】


start
APリストの消去
S101
スキャンおよびAPのサーチ
S103
APリストの送信
S105
所定の待機時間（ｔ）を待機
S107

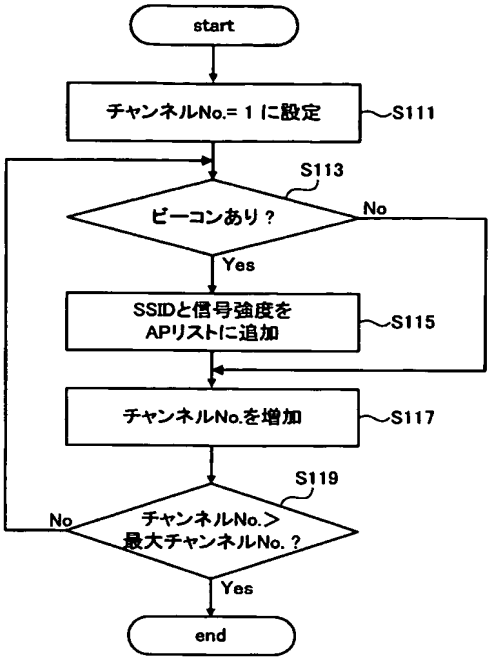
【図２】


10a～e（クライアント）
演算処理部
11
メモリ
12
HDD
13
APリスト記憶部
19
入出力部
14
送受信部
15
APサーチ部
16
APリスト送出部
17
18

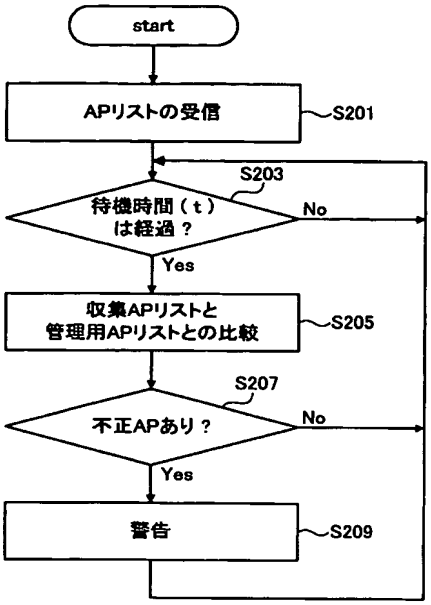
【図３】


20（コントローラ）
演算処理部
21
APリスト比較処理部
26
メモリ
22
HDD
23
APリスト登録部
27
入出力部
24
送受信部
25
APリスト受信部
28

【図５】



【図６】



【図７】

（ａ）

クライアント名	APリスト
クライアント10a	A、B
クライアント10b	A、B、C
クライアント10c	B、C
クライアント10d	C、D
クライアント10e	D

→ 集収APリスト

A、B、C、D

（ｂ）

集収APリスト	A、B、C、D
登録APリスト	A、B、D

フロントページの続き

(72)発明者　藤井　一男
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内
(72)発明者　松永　幸三
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内
(72)発明者　伊藤　雅晴
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

Ｆターム(参考)　5K033 AA08 CB01 DA01 DA17 DB20
5K067 AA30 BB21 DD19 EE02 EE10
EE16 FF03 HH23 KK15